Every cyclic group is abelian.

Let $(G, *)$ be a cyclic group then $\langle a \rangle = G$ for some $a \in G$.

That is, $G = \{a, a^2, \ldots, a^n = e\}$

Let $b, c \in G$. Then to show $b * c = c * b$ for abelian

$\because b \in G \Rightarrow b = a^m$ for some m

& $c \in G \Rightarrow c = a^p$ for some p

$\therefore b * c = a^m * a^p = a^{m+p} = a^{p+m} = a^p * a^m = c * b$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, with addition modulo n is a cyclic group of order n. So, this is an example of cyclic group of any finite order.

<u>Permutation group</u>: A permutation of a set A is a function form A to A that is both one-one and onto.

A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Let $S = \{1, 2, 3\}$ be a set then there are $3!$ functions which are one-one & onto on S. And the functions are

$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

I $\quad (12) \quad (13) \quad (23) \quad (123) \quad (132)$

$\alpha(1) = 1$, $\alpha(2) = 2$, $\alpha(3) = 3$; $\beta(1) = 2$, $\beta(2) = 1$, $\beta(3) = 3$

$\gamma(1) = 1$, $\gamma(2) = 2$, $\gamma(3) = 1$; ...

$\alpha \circ \beta(1) = \alpha(2) = 2$

$\alpha \circ \beta(2) = \alpha(1) = 1$

$\alpha \circ \beta(3) = \alpha(3) = 3$

In short,

$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta$

The permutation I is identity element of S_3 (Permutation group)

Inverse $(12)\circ(12) = I \Rightarrow |(12)| = 2$ & $(12)^{-1} = (12)$

$(13)\circ(13) = I \Rightarrow (13)^{-1} = (13)$ & $|(13)| = 2$

$(23)\circ(23) = I \Rightarrow (23)^{-1} = (23)$ & $|(23)| = 2$

$(123)\circ(132) = I \Rightarrow (123)^{-1} = (132)$ & vice versa

$(123)\circ(123)\circ(123) = I \Rightarrow |(123)| = 3.$

And $(12)\circ(13) = (132)$ & $(13)\circ(12) = (123)$

$\therefore (12)\circ(13) \neq (13)\circ(12)$

$\therefore$ The permutation group is non-Abelian $\forall\, n \geq 3$.

The symmetric groups (Permutation groups) are rich in subgroups. The group S_4 has 30 subgroups and S_5 has well over 100 subgroups.

group table (Cayley table) for S_3

	I	(12)	(13)	(23)	(123)	(132)
I	I	(12)	(13)	(23)	(123)	(132)
(12)	(12)	I	(132)	(123)	(23)	(13)
(13)	(13)	(123)	I	(132)	(12)	(23)
(23)	(23)	(132)	(123)	I	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	I
(132)	(132)	(23)	(12)	(13)	I	(123)

Subgroups are $\{I\}$, S_3, $\{I, (12)\}$, $\{I, (13)\}$, $\{I, (23)\}$, $\{I, (123), (132)\}$

(6)

→ Every permutation is a product of 2-cycles (transpositions)

consider a permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} = \underbrace{(1\,2)}_{\text{2-cycle}}\underbrace{(3\,4\,6)}_{\text{3-cycles}}$

$(1\,2)(3\,4\,6) = (1\,2)(3\,4)(3\,6)$

→ If the pair of cycles α and β have no entries in common, then $\alpha\beta = \beta\alpha$.

→ The order of a permutation in disjoint cycle form is the LCM of the lengths of the cycles.

consider element $(1\,2)(3\,4\,6) \in S_6$. This element has two cycles (disjoint cycles). The first cycle $(1\,2)$ has two entries, so its length is 2. The second cycle $(3\,4\,6)$ is of length 3. Therefore, the order of $(1\,2)(3\,4\,6)$ is $LCM(2,3) = 6$.

→ A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation.

A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.

$(1\,2)(3\,4\,6) = (1\,2)(3\,6)(3\,4)$ → odd permutation

$(1\,2)(3\,4)$ → even

$(1\,2\,3) = (1\,3)(1\,2)$ → even

$(1\,2)$ → odd

→ The set of even permutations in S_n forms a subgroup of S_n. And the subgroup A_n is called alternating group of order $\frac{n!}{2}$.

$A_3 = \{I, (1\,2\,3), (1\,3\,2)\}$ is subgroup of S_3

$A_4 = \{I, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (2\,4\,3), (1\,4\,2), (1\,3\,4), (1\,3\,2), (1\,4\,3), (2\,3\,4), (1\,2\,4)\}$ is subgroup of S_4.